Listing of Claims:

1. (Original)   A password management system comprising:

a host computing processor having a peripheral port, and operable to encrypt a list of passwords; and

a portable access device adapted to be coupled to the host computing processor, the portable access device storing the list of encrypted passwords, and communicating the list of encrypted passwords with the host computing processor through the peripheral port.

2. (Original)   The system of claim 1, wherein the portable access device further comprises a rewritable memory configured to store the list of encrypted passwords and account data associating each password, and configured to overwrite the list of passwords with a modified list of passwords.

3. (Original)   The system of claim 1, wherein the portable access device comprises a first rewritable memory bank configured to store the list of encrypted passwords and account data associating each password, and a second rewritable memory bank configured to duplicate information stored in the first memory bank.

4. (Original)   The system of claim 1, wherein the peripheral port comprises a universal serial bus ("USB") port.

5. (Original)   The system of claim 4, wherein the portable access device comprises a serial interface circuitry configured to communicate with the host computing processor via the USB port.

6. (Original)   The system of claim 1, further comprising a data flow drive coupling the portable access device to the peripheral port of the host computing processor, being operable to read from the portable access device, and being operable to write to the portable access device.

7. (Original)   The system of claim 1, wherein the host computing processor comprises an encryption module configured to encrypt the list of passwords.

8. (Original)   The system of claim 7, wherein the encryption module comprises a symmetric encryption program.

9. (Original)   The system of claim 1, further comprising a driver configured to read a master access code and to decrypt the list of passwords with the master access code.

10. (Original) The system of claim 1, further comprising a driver configured to update the list of encrypted passwords.

11. (Original) The system of claim 1, further comprising a driver configured to perform error correction on the list of passwords.

12. (Original) A password management system operable to be coupled to a computer having access to at least one account, the at least one account having a password associated therewith, the password management system comprising:

a portable access device storing in a rewritable memory a list of encrypted passwords for the at least one account;

an encryption module executed on the computer and operable to encrypt a new password for addition to the list of passwords; and

a driver coupled to the encryption module and operable to read a master access code, the driver decrypting the list of encrypted passwords from the portable access device using the master access code and updating the list of encrypted passwords with the new encrypted password.

13. (Original) The system of claim 12, wherein the rewritable memory comprises a first rewritable memory bank configured to store the list of encrypted passwords and account data associating each password, and a second rewritable memory bank configured to duplicate information stored in the first memory bank.

14. (Original) The system of claim 12, wherein the portable access device couples to the computer via a peripheral port.

15. (Original) The system of claim 14, wherein the peripheral port comprises a universal serial bus ("USB") port.

16. (Original) The system of claim 15, wherein the portable access device comprises a serial interface circuitry configured to communicate with the computer via the USB port.

17. (Original) The system of claim 12, further comprising a data flow drive coupling the portable access device to the computer, being operable to read from the portable access device, and being operable to write to the portable access device.

18. (Original) The system of claim 12, wherein the encryption module comprises a symmetric encryption program.

19. (Original) The system of claim 12, wherein the driver performs error correction on the list of passwords.

20. (Original) A method of managing a list of passwords, the method comprising:

encrypting a list of passwords at a host computing processor;

storing the list of encrypted passwords at a portable access device selectively coupled to the host computing processor; and

communicating the at least one encrypted password between the host computing processor and the portable access device.

21. (Original) The method of claim 20, wherein the portable access device further comprises a rewritable memory configured to store the list of encrypted passwords, and account data associating each password.

22. (Original) The method of claim 20, further comprising:

storing the list of encrypted passwords at a first memory bank of the portable access device; and

copying the list of encrypted passwords from the first memory bank to a second memory bank of the portable access device.

23. (Original) The method of claim 20, wherein communicating the list of encrypted passwords between the host computing processor and the portable access device comprises communicating with a peripheral port of the host computer processor, wherein the peripheral port comprises a universal serial bus ("USB") port.

24. (Original) The method of claim 23, further comprising interfacing between the host computing processor and the portable access device using a serial interface circuitry on the portable access device via the USB port.

25. (Original) The method of claim 20, further comprising:

controlling data flow between the portable access device and the host computing processor;

reading from the portable access device a list of encrypted passwords; and

writing to the portable access device a list of encrypted passwords.

26. (Original) The method of claim 20, wherein encrypting the list of passwords comprises using a symmetric encryption program.

27. (Original) The method of claim 20, further comprising:

reading a master access code; and

decrypting the list of passwords with the master access code.

28. (Original) The method of claim 20, further comprising updating the list of encrypted passwords.

29. (Original) The method of claim 20, further comprising performing error correction on the list of passwords.